Application for United States Letters Patent

FOR ATTORNEY DOCKET NUMBER SDT-040 (7216/55)

TO ALL WHOM IT MAY CONCERN:

Be it known that we, William Duane, and Peter Röstin, have invented

SYSTEM AND METHODS FOR MAINTAINING AND DISTRIBUTING
PERSONAL SECURITY DEVICES

of which the following is a specification.

SYSTEM AND METHODS FOR MAINTAINING AND DISTRIBUTING PERSONAL SECURITY DEVICES

BACKGROUND OF THE INVENTION

Field of the Invention

This invention relates to the field of cryptography, including user authentication, document authentication, symmetric key cryptography, public key cryptography, secure communications, secret sharing, and key distribution.

Description of the Related Art

Cryptography has become increasingly important with the increased presence of the Internet, an inherently insecure transmission medium. Cryptography enables methods of secure user authentication, which is a prerequisite to performing secure electronic commerce on the Internet.

Typical methods of user authentication are insecure and vulnerable to eavesdropping. For example, suppose that a user Alice wishes to log into a computer over the Internet. A typical authentication process requires Alice to enter her password. This password is typically entered and transmitted in the clear and may be easily intercepted by an eavesdropper Eve as it travels across the Internet, providing Eve with the information necessary to gain exactly the same access privileges as Alice. Cryptography provides secure authentication protocols allowing Eve to eavesdrop on the authentication information without providing her with the necessary information to gain the same access privileges as Alice.

Cryptographic methods of secure user authentication require the storage of sensitive information, typically on a medium such as the hard disk drive of a general purpose computer or the flash memory of a personal digital assistant. With the increasing portability and mobility of such hardware comes the increasing ease of its theft. In one illustrative example, a user travels with a laptop computer containing authentication information stored on its hard disk. This authentication information can be used to make a secure network connection, to log in to a remote host, and to sign email. If the laptop were to be stolen, the thief could then use this stolen information to perform further mischief by masquerading as the user.

One type of sensitive authentication information is a user's private key. A private key is a component of public key cryptography, which enables methods of user authentication as well as secure communications over unsecured channels. Public key cryptography employs a key pair comprising a public key and a private key. One key is used to encrypt a file and the other key is used to decrypt it. The key used to encrypt a file is not useful for subsequently decrypting it. In general, public key cryptography enables a user Alice to authenticate herself to another user Bob by encrypting data provided by Bob with her private key, creating a digital signature. Alice then sends the signature to Bob. Bob then uses Alice's public key to decrypt the signature, which he then compares to the plaintext. Alice is authenticated to Bob if the decrypted and plaintext data match. Implementations of public key cryptography include RSA, Diffie-Helman, ElGamal, and Elliptic Curve Cryptography ("ECC").

Another type of sensitive information is the output of an authentication token. In one implementation, an authentication token displays a number that changes periodically. The numbers displayed are elements in a pseudorandom sequence. Before the token is used, it is synchronized with a security server so that the security server subsequently knows what number is displayed on the token at any given time. When a user seeks access to a resource administered by the security server, the user sends the server the number currently displayed on the token. The server then authenticates the user by comparing the sent number with the number that the server expects the authentication token to currently display. If they match, the user is authenticated and granted access to

the resource. An authentication token can be implemented in hardware or software. In one software implementation, an authentication token includes program code running on the user's laptop.

Another type of sensitive information is a key to a challenge-response protocol. In one implementation of this protocol, the key comprises a number known by the user and an authentication server. Instead of requesting the number directly, the authentication server sends the user an operand. The user performs a mathematical function using the operand and the key and sends the result back to the authentication server, which compares the user's answer with the expected answer. The mathematical function is designed so that it is impractical to discern the key from the operand and the result. A challenge-response authentication protocol can be implemented in software on the user's a general purpose computer.

Sensitive information for secure user authentication can be stored on a variety of hardware. For example, secure user authentication methods may be implemented on a workstation, a desktop computer, a laptop computer, a personal digital assistant, a smartcard, a universal serial bus ("USB") key, or specialized hardware. This specialized hardware can be small and portable, with form factors similar to a credit card, a gumdrop, or a school ring.

There is a need to protect sensitive information stored on a wide range hardware that is subject to several forms of physical compromise.

BRIEF SUMMARY OF THE INVENTION

The invention provides apparatus and methods for securely accessing and providing information. In one embodiment the invention relates to a method for securely providing information including the steps of receiving information identifying an encrypted personal security device, providing the encrypted personal security device, receiving authentication information, and providing decryption information for the personal security device responsive to the authentication information. In a further embodiment, the encrypted personal security device includes an encrypted key. In another embodiment, the encrypted personal security device includes information

necessary to make a secure virtual private network connection. In another embodiment. the method further includes the step of validating the authentication information. In another embodiment, the step of providing the encrypted personal security device includes the steps of retrieving and providing the personal security device. In a further

5 embodiment, the retrieval step includes retrieving the personal security device from an authentication server. In another embodiment, the method further includes the step of storing the personal security device on a smartcard. In another embodiment, the method further includes the step of storing the personal security device in a volatile memory element.

10 In another aspect the invention relates to a method for accessing secure information including the steps of receiving an encrypted personal security device, receiving decryption information for the personal security device, and decrypting the personal security device. In one embodiment the method further includes the step of using the decrypted personal security device to access secure information. In another

15 embodiment, the personal security device includes information necessary to make a secure network connection between a network client and a network server. In another embodiment, the personal security device includes information necessary to make a secure virtual private network connection. In another embodiment, the method further includes the steps of transmitting information identifying an encrypted personal security

20 device and transmitting authentication information. In another embodiment, the method further includes the step of storing the personal security device on a smartcard. In another embodiment, the method further includes the step of storing the personal security device in a volatile memory element.

In another embodiment the invention relates to a method for allowing a network

25 client secure access to information including the steps of requesting, by the network client, a personal security device from a network server, wherein the personal security device includes encrypted information necessary to make a secure network connection, forwarding, by the network server, the personal security device to the network client, and providing, by the network server, decryption information for the personal security device.

30 In another embodiment, the personal security device includes information necessary to

make a secure virtual private network connection. In another embodiment, the method further includes the steps of forwarding, by the network server, the request to an authentication server, querying, by the authentication server, a user databse with the request, returning, by the user database, a personal security device to the authentication server, and forwarding, by the authentication server, the personal security device to the network server. In another embodiment, the method further includes the steps of obtaining, by the client, authentication information from an authentication token, providing, by the client, the authentication information to the authentication server, confirming, by the authentication server, the validity of the authentication information, retrieving, by the network server, decryption information for the personal security device from a database, and providing, by the network server, decryption information for the personal security device to the client. In another embodiment, the method further includes the step of decrypting, by the client, the personal security device.

In another embodiment the invention relates to a device for providing secure access to information including a first receiver receiving information identifying an encrypted personal security device, a first transmitter providing the personal security device, a second receiver receiving authentication information, and a second transmitter providing decryption information for the personal security device responsive to the authentication information. In a further embodiment, the personal security device includes an encrypted key. In another embodiment, the personal security device includes information necessary to make a secure network connection between a network client and a network server. In another embodiment, the personal security device includes information necessary to make a secure virtual private network connection. In another embodiment, the device also includes an authenticator validating the authentication information. In another embodiment, the first receiver is the same as the second receiver. In another embodiment, the first transmitter is the same as the second transmitter.

In another aspect the invention relates to a device for accessing secure information including a first receiver receiving an encrypted personal security device, a second receiver receiving decryption information for the personal security device, and a decryptor decrypting the personal security device. In another embodiment, the personal

security device includes information necessary to make a secure network connection between a network client and a network server. In another embodiment, the personal security device includes information necessary to make a secure virtual private network connection. In another embodiment, the device further includes a first transmitter

5   transmitting information identifying an encrypted personal security device, and a second transmitter transmitting authentication information. In another embodiment, the first transmitter is the same as the second transmitter. In another embodiment, the device also includes a smartcard storing the decryption information. In another embodiment, the device also includes a volatile memory element storing the decryption information. In

10   another embodiment, the first receiver is the same as the second receiver.

In another embodiment the invention relates to a system for providing secure access to information including a network client including a volatile memory element and a network server storing an encrypted personal security device in a server memory element, the personal security device including encrypted information. In another

15   embodiment, the system further includes a smartcard having a volatile memory element storing the personal security device. In another embodiment, the system further includes decrypted information for forming a secure network connection between the client and the server wherein the decrypted information is derived from applying the decryption information to the personal security device. In a further embodiment, the decryption

20   information is stored in the volatile memory element. In a further embodiment, the decrypted information is stored in the volatile memory element. In another embodiment, the network is a virtual private network. In a further embodiment, the encrypted information includes information necessary for forming a secure network connection the the client and the server. In a further embodiment, the system further includes an

25   authentication token, wherein the token is capable of providing authentication information, and an authentication server, wherein the authentication server includes a user database, wherein the user database includes decryption information for the personal security device, and wherein the authentication server is capable of providing the decryption information upon receipt of the authentication information.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

The foregoing and other objects, features and advantages of the present invention, as well as the invention itself, will be more fully understood from the following description of preferred embodiments, when read together with the accompanying drawings, in which:

FIG. 1 is a flowchart illustrating the interaction between a client and a server.

FIG. 2 is a flowchart illustrating steps a server undertakes to securely provide information.

FIG. 3 is a flowchart illustrating steps a client undertakes performing a challenge-response protocol for accessing information.

FIG. 4 is a schematic illustration of a security regime.

FIG. 5 is a flowchart illustrating steps a client undertakes to securely receive and access information.

FIG. 6 is a schematic illustration of a hardware embodiment used to store and access a personal security device.

FIG. 7 is a schematic illustration of a hardware embodiment used to store and access a personal security device.

FIG. 8 is a flowchart illustrating steps to erase sensitive information after use.

FIG. 9 is a schematic illustration of a system for securely providing information.

FIG. 10 is a schematic illustration of a workstation storing and decrypting a personal security device.

FIG. 11 is a schematic illustration of a system for securely providing a key in response to authentication.

FIG. 12 is a schematic illustration of a smartcard and a smartcard reader.

FIG. 13 is a schematic illustration of a personal security device stored in an external non-volatile medium.

DETAILED DESCRIPTION OF THE INVENTION

For the purposes of this invention, the term "personal security device" refers to encrypted sensitive information that may be stored on devices subject to physical

compromise. "Personal security device" may also be used as a synecdoche to refer to the hardware storing this encrypted sensitive information. In one embodiment of the invention, the personal security device can only be decrypted with decryption information, known as a key.

5   For the purposes of this invention, "non-volatile storage medium" refers to any medium in which data persists when power is not supplied to the device on which the medium resides. Examples of non-volatile storage media include disks, tapes, compact disc read-only memory ("CD-ROM"), digital versatile disc ("DVD"), flash memory, erasable-programmable read-only memory ("EPROM") and read-only memory ("ROM").

10   For the purposes of this invention, "volatile storage medium" refers to any medium in which data is stored in a transitory manner or data is lost when power is removed from the medium. An example of a volatile storage medium is random-access memory ("RAM"). In a typical embodiment, volatile storage media are less susceptible to physical compromise than non-volatile storage media.

15   For the purposes of this invention, the term "physical compromise" encompasses any means by which an adversary may gain access to information on a user's system. For example, a laptop computer can be stolen and its contents accessed. Physical compromise also encompasses an adversary may gaining entrance to an office and copying sensitive contents of a target computer onto a removable storage medium such as

20   a floppy disk or removable cartridge. Physical compromise also encompasses an adversary transmitting sensitive information from a target computer to one of the adversary's computers over a computer network such as the Internet. Physical compromise also encompasses the use of cracking methods including viruses and trojan horses. For example, a desktop system can be infected with a virus that seeks out

25   sensitive information and transmits what it finds to an adversary over the Internet. Alternatively, an adversary can exploit a security hole in an operating system to gain access to that system directly. One example of a security hole exploit is known as Back Orifice, which provides unauthorized access to systems running Microsoft's Windows NT operating system.

For the purposes of this invention, the term "authentication token" refers to a device or program providing authentication information to a user that is determined based on secret information shared by the authentication token and an authentication server. In one embodiment, the authentication token is implemented as code running on the user's general purpose computer. In an alternate embodiment, the authentication token is implemented on specialized hardware.

Referring to FIG. 1, and in brief overview, a system is provided

One embodiment of the invention, as illustrated in FIG. 1, includes a client that interacts with a server to gain access to sensitive information. The client first transmits a personal security device query to the server (Step 100). In one embodiment, this query includes information necessary to uniquely identify a specific personal security device. In an alternate embodiment, the query includes a request to generate a new personal security device. In one embodiment, the query is received via a computer network. In a further embodiment, the computer network is a local area network. In an alternate embodiment, the computer network is a wide area network. In a further embodiment, the wide area network is the Internet. In one embodiment, the query is received via an open or unsecured connection. In an alternate embodiment, the query is received via a secured connection. In a further embodiment, the connection is secured by the SSL protocol. In one embodiment, the query does not include any authentication information.

The server receives the personal security device query (Step 110), and provides the personal security device to the client (Step 120). In one embodiment, the server provides the personal security device by transmitting it over a computer network. In a further embodiment, the computer network is a local area network. In an alternate embodiment, the computer network is a wide area network. In a further embodiment, the wide area network is the Internet. In one embodiment, the personal security device is transmitted over an open or unsecured connection. In an alternate embodiment, the personal security device is transmitted over a secured connection. In a further embodiment, the connection is secured by the SSL protocol.

The client then receives the transmitted personal security device (Step 130) and transmits a key query requesting the key to the personal security device (Step 140). The

key query includes an unique identifier for the personal security device to be decrypted. The key query also includes authentication information. In one embodiment, the authentication information is the output of an authentication token. In an alternate embodiment, the authentication information is a digitally-signed document. In yet another alternate embodiment, the authentication information is a passphrase. In yet another alternate embodiment, the authentication information is a response to a challenge. In yet another alternate embodiment, the authentication information includes biometric information. In one embodiment, the key query is transmitted via a computer network. In a further embodiment, the computer network is a local area network. In an alternate embodiment, the computer network is a wide area network. In a further embodiment, the wide area network is the Internet. In one embodiment, the key query is transmitted via an open or unsecured connection. In an alternate embodiment, the key query is transmitted via a secured connection. In a further embodiment, the connection is secured by the SSL protocol.

The server then receives the key query (Step 150) and determines if the authentication information is correct (Step 160). In one embodiment, the server determines if the authentication information matches the information the server expects to be displayed on an authentication token. In an alternate embodiment, the server verifies the authentication information's digital signature. In yet another alternate embodiment, the server determines if the authentication information matches a passphrase. In yet another alternate embodiment, the server determines if the authentication information is a correctly calculated response to a challenge. In yet another alternate embodiment, the server determines if the authentication information matches a user's biometric information.

If the authentication information is correct, the server provides the key to the personal security device (Step 170). Otherwise the server refuses to provide the key (Step 180). In one embodiment, the server provides the key by transmitting it over a computer network. In a further embodiment, the computer network is a local area network. In an alternate embodiment, the computer network is a wide area network. In a further embodiment, the wide area network is the Internet. In one embodiment, the key is

transmitted over an open or unsecured connection. In an alternate embodiment, the key is transmitted over a secured connection. In a further embodiment, the connection is secured by the SSL protocol.

The client receives the key (Step 190) and uses it to decrypt the personal security device (Step 195) thereby gaining access to its contents. In one embodiment, the key is a symmetric key and decryption is performed using a symmetric cipher such as RC4, A4, DES, RC5, Blowfish, or RC6. In an alternate embodiment, the key is a first asymmetric key of a key pair, the personal security device was encrypted with a second key of a key pair, and the decryption is performed using a public-key cryptographic cipher.

In one embodiment of this invention, the personal security device may be distributed openly and without any requirement for authentication. In a further embodiment, the key to the personal security device is not distributed openly, but only in response to proper authentication. FIG. 2 illustrates steps taken by a server of this embodiment. The server receives a query for a personal security device (Step 200). In one embodiment, this query includes information necessary to uniquely identify a specific personal security device. In an alternate embodiment, the query includes a request to generate a new personal security device. In one embodiment, the query is received via a computer network. In a further embodiment, the computer network is a local area network. In an alternate embodiment, the computer network is a wide area network. In a further embodiment, the wide area network is the Internet. In one embodiment, the query is received via an open or unsecured connection. In an alternate embodiment, the query is received via a secured connection. In a further embodiment, the connection is secured by the SSL protocol. In one embodiment, the query does not include any authentication information.

The server then provides the personal security device (Step 210). In one embodiment, the server provides the personal security device by transmitting it over a computer network. In a further embodiment, the computer network is a local area network. In an alternate embodiment, the computer network is a wide area network. In a further embodiment, the wide area network is the Internet. In one embodiment, the personal security device is transmitted over an open or unsecured connection. In an

-12-

alternate embodiment, the personal security device is transmitted over a secured connection. In a further embodiment, the connection is secured by the SSL protocol.

The server then receives a key query (Step 220). The key query includes an unique identifier for the personal security device to be decrypted. The key query also includes authentication information. In one embodiment, the authentication information is the output of an authentication token. In an alternate embodiment, the authentication information is a digitally-signed document. In yet another alternate embodiment, the authentication information is a passphrase. In yet another alternate embodiment, the authentication information is a response to a challenge. In yet another alternate embodiment, the authentication information includes biometric information. In one embodiment, the key query is received via a computer network. In a further embodiment, the computer network is a local area network. In an alternate embodiment, the computer network is a wide area network. In a further embodiment, the wide area network is the Internet. In one embodiment, the key query is received via an open or unsecured connection. In an alternate embodiment, the key query is received via a secured connection. In a further embodiment, the connection is secured by the SSL protocol.

The server then determines if the authentication information is correct (Step 230). In one embodiment, the server determines if the authentication information matches the information the server expects to be displayed on an authentication token. In an alternate embodiment, the server verifies the authentication information's digital signature. In yet another alternate embodiment, the server determines if the authentication information matches a passphrase. In yet another alternate embodiment, the server determines if the authentication information is a correctly calculated response to a challenge. In yet another alternate embodiment, the server determines if the authentication information matches a user's biometric information.

If the authentication information is correct, the server provides the key to the personal security device (Step 240). Otherwise the server refuses to provide the key (Step 250). In one embodiment, the server provides the key by transmitting it over a computer network. In a further embodiment, the computer network is a local area network. In an alternate embodiment, the computer network is a wide area network. In a further

-13-

embodiment, the wide area network is the Internet. In one embodiment, the key is transmitted over an open or unsecured connection. In an alternate embodiment, the key is transmitted over a secured connection. In a further embodiment, the connection is secured by the SSL protocol.

Methods of providing proper authentication include but are not limited to entering a password, successfully completing a challenge-response protocol, entering data from an authentication token, and biometric authentication. Characterisitics for biometric authentication can include fingerprints, voice prints, retinal scan, facial features, or the measurement of any physical characteristic associated with a user to be authenticated.

FIG. 3 illustrates an embodiment employing a challenge-response protocol. A client requests a specific personal security device by sending a personal security device query (Step 300). In one embodiment, this query includes information necessary to uniquely identify a specific personal security device. In an alternate embodiment, the query includes a request to generate a new personal security device. In one embodiment, the query is received via a computer network. In a further embodiment, the computer network is a local area network. In an alternate embodiment, the computer network is a wide area network. In a further embodiment, the wide area network is the Internet. In one embodiment, the query is received via an open or unsecured connection. In an alternate embodiment, the query is received via a secured connection. In a further embodiment, the connection is secured by the SSL protocol. In one embodiment, the query does not include any authentication information.

The client then receives the personal security device (Step 310). In one embodiment, the client receives the personal security device over a computer network. In a further embodiment, the computer network is a local area network. In an alternate embodiment, the computer network is a wide area network. In a further embodiment, the wide area network is the Internet. In one embodiment, the personal security device is received over an open or unsecured connection. In an alternate embodiment, the personal security device is received over a secured connection. In a further embodiment, the connection is secured by the SSL protocol.

-14-

The client then requests the key to the personal security device by transmitting a key query (Step 320). The key query includes an unique identifier for the personal security device to be decrypted. In one embodiment, the key query is transmitted via a computer network. In a further embodiment, the computer network is a local area

5 network. In an alternate embodiment, the computer network is a wide area network. In a further embodiment, the wide area network is the Internet. In one embodiment, the key query is transmitted via an open or unsecured connection. In an alternate embodiment, the key query is transmitted via a secured connection. In a further embodiment, the connection is secured by the SSL protocol.

10 Next, the client receives an authentication challenge (Step 330). In one embodiment, the authentication challenge is an operand generated by the server, where the proper response is the result of performing a mathematical function on the operand and a secret number. In a further embodiment, the mathematical function is a one-way function, such that it is infeasible to determine the secret number from the operand and

15 the result. In one embodiment, the authentication challenge is received via a computer network. In a further embodiment, the computer network is a local area network. In an alternate embodiment, the computer network is a wide area network. In a further embodiment, the wide area network is the Internet. In one embodiment, the authentication challenge is received via an open or unsecured connection. In an alternate

20 embodiment, the authentication challenge is received via a secured connection. In a further embodiment, the connection is secured by the SSL protocol.

Next, the client provides a response to the authentication challenge (Step 340). In one embodiment, the response is generated by performing the mathematical function on the operand and the secret number. In one embodiment, the client provides the response

25 by transmitting it over a computer network. In a further embodiment, the computer network is a local area network. In an alternate embodiment, the computer network is a wide area network. In a further embodiment, the wide area network is the Internet. In one embodiment, the response is transmitted over an open or unsecured connection. In an alternate embodiment, the response is transmitted over a secured connection. In a further

30 embodiment, the connection is secured by the SSL protocol.

The response is then validated (Step 350). If the response is authentic, then the client is send the key (Step 370) which the client then uses to decrypt the personal security device (Step 380) and gain access to its contents. If the response is not authentic, then the client is refused the key (Step 360). In one embodiment, the key is a symmetric key and decryption is performed using a symmetric cipher such as RC2, RC5, DES, Twofish, A5, or RC4. In an alternate embodiment, the key is a first asymmetric key of a key pair, the personal security device was encrypted with a second key of a key pair, and the decryption is performed using a public-key cryptographic cipher such as RSA, Diffie-Helman, ElGamal or Elliptic Curve Cryptography ("ECC"). In one embodiment, the key is received via a computer network. In a further embodiment, the computer network is a local area network. In an alternate embodiment, the computer network is a wide area network. In a further embodiment, the wide area network is the Internet. In one embodiment, the key is received via a secured connection. In a further embodiment, the connection is secured by the SSL protocol.

The personal security device server does not have to be the same as the authentication server. The embodiment in FIG. 4 illustrates the separation of the personal security device server 400 from the authentication server 410. The personal security device server 400 is in operative association with a personal security device database 420. The personal security device server 400 provides the contents of the personal security device database 420 without requiring authentication. In this embodiment, the contents of the personal security device database 420 can be considered public information. The authentication server 410 is in operative association with a key database 430. The information in the key database 430 is sensitive information which must be kept secure and is only given out in response to proper authentication. Optionally, the authentication server 410 and the key database 430 can be further protected by being placed behind a firewall 440.

In one embodiment of the invention, a user requests and receives a personal security device from a server, which the user then stores in a non-volatile storage medium such as a hard disk drive or flash memory. In a further embodiment, the user requests the key to the personal security device while providing proper authentication. In this

-16-

embodiment, the user stores the key in a volatile storage medium, such as random access memory ("RAM"). In yet a further embodiment, the user decrypts the personal security device with the key and stores the decrypted sensitive information in a volatile storage medium. FIG. 5 illustrates the steps taken by a user or client of this embodiment. The client receives a personal security device (Step 500). In one embodiment, the client receives the personal security device over a computer network. In a further embodiment, the computer network is a local area network. In an alternate embodiment, the computer network is a wide area network. In a further embodiment, the wide area network is the Internet. In one embodiment, the personal security device is received over an open or unsecured connection. In an alternate embodiment, the personal security device is received over a secured connection. In a further embodiment, the connection is secured by the SSL protocol.

The personal security device is then stored on the client on a non-volatile storage medium (Step 510). In one embodiment, the non-volatile storage medium is a disk drive such as a hard disk, a floppy disk, or a removable cartridge such as a Zip drive. In an alternate embodiment, the non-volatile storage medium is memory such as flash memory or eraseable programmable read-only memory ("EPROM") where the contents of the memory are retained even if power is removed.

The client then receives the key to the personal security device (Step 520), typically in response to successful authentication. In one embodiment, the key is received via a computer network. In a further embodiment, the computer network is a local area network. In an alternate embodiment, the computer network is a wide area network. In a further embodiment, the wide area network is the Internet. In one embodiment, the key is received via a secured connection. In a further embodiment, the connection is secured by the SSL protocol.

The client then uses the key to decrypt the personal security device and gain access to its contents (Step 530). In this embodiment, the key and the decrypted contents are stored in the client's volatile storage medium. In one embodiment, the key is a symmetric key and decryption is performed using a symmetric cipher. In an alternate embodiment, the key is a first asymmetric key of a key pair, the personal security device

-17-

was encrypted with a second key of a key pair, and the decryption is performed using a public-key cryptographic cipher.

FIG. 6 illustrates the hardware of an embodiment used to store and access a personal security device and its contents. The hardware includes a central processing unit ("CPU") 600 in operative association with volatile storage 610 and non-volatile storage 620. In this embodiment, an encrypted personal security device 630 is stored in the non-volatile storage 610. When a user wishes to access the contents of the personal security device 630, a key 640 is stored in the volatile storage 610. The CPU 600 then uses the key 640 to decrypt the contents of the personal security device and store the decrypted contents 650 in the volatile storage 610.

Some general purpose computers use non-volatile disk storage to supplement volatile random access memory ("RAM") storage. Referring to FIG. 7, a general purpose computer 700 includes a central processing unit ("CPU") 710 in operative association with volatile RAM 720 and a non-volatile disk drive 740. The disk drive 740 includes swap space 730. When sections of RAM 720 aren't being used, their contents are "swapped out" into the swap space 730 so that the RAM 720 can be used for other purposes. When a user wishes to access those contents, they are swapped back into the RAM 720. Because the use of swap space 730 writes the contents of volatile storage 720 into non-volatile storage 740, it is desirable to erase sensitive information from volatile storage 720 as soon as it is finished being used. Otherwise, unused sensitive information could be written out to nonvolatile swap space 730.

In one embodiment, illustrated in the flowchart of FIG. 8, the information stored in the volatile storage medium is erased after use. First, the personal security device is stored in a non-volatile storage medium (Step 800). In one embodiment, the personal security device is stored by a user after having been provided by a server. In an alternate embodiment, the personal security device is stored in the non-volatile storage medium before the medium is distributed to the user.

Next, the key to the personal security device is stored in a volatile medium (Step 810). In one embodiment, the key is obtained from an authentication server. In an alternate embodiment, the key is directly entered by a user.

-18-

The key is then used to decrypt the personal security device (Step 820). In one embodiment, the key is a symmetric key and decryption is performed using a symmetric cipher. In an alternate embodiment, the key is a first asymmetric key of a key pair, the personal security device was encrypted with a second key of a key pair, and the decryption is performed using a public-key cryptographic cipher. The decrypted contents of the personal security device are stored in volatile memory (Step 830).

After being used to perform decryption, the key is erased from volatile memory (Step 840). In one embodiment, the key is erased by zeroing out the memory location where the key was stored. If this memory location is subsequently swapped out, the key will not be stored on a non-volatile medium.

The user then uses the decrypted contents of the personal security device (Step 850). After the user is finished with the contents, the contents are erased from volatile memory (Step 860). In one embodiment, the contents are erased by zeroing out the memory location where the contents were stored. If this memory location is subsequently swapped out, the contents will not be stored on a non-volatile medium. If the user wishes to subsequently use the contents (Step 850), Steps 810-840 must be repeated.

The encrypted sensitive information stored in a personal security device may include, but is not limited to, information necessary for forming a secure network connection, user authentication information, a symmetric encryption key, a private key, a public key certificate, a password or passphrase, contact information such as a name and address, a credit card number, an account number with a financial institution, a personal identification number ("PIN"), a medical record, biometric information, a transaction record, and a map revealing the location of a resource, or combinations thereof. A secure network connection may include a virtual private network ("VPN") connection. The information necessary for forming a secure network connection may include, but is not limited to, a symmetric encryption key and a private key.

In one embodiment, known as symmetric key wrapping, a personal security device includes a symmetrically encrypted file along with the symmetric key used to encrypt it. In this embodiment, the symmetric key is itself encrypted by a second key,

which may be a symmetric or a public or private key. This second key is the key to the personal security device of this embodiment.

Example 1

In this example, which is illustrated in FIG. 9, a user wishes to use a computer 900 to present credentials 910 such as a public key certificate or a digitally signed document to a host 920. The user first obtains a personal security device 930 from a personal security device server 940. In this embodiment, the personal security device 930 includes the user's encrypted credentials. The personal security device server 940 includes a personal security device database 950. The user then retrieves authentication information 960 from a token 970 and provides the authentication information 960 to an authentication server 980. The authentication server 980 is in operative association with a key database 990. If the authentication server 980 determines that the authentication information 960 is correct, the authentication server 980 then provides a key 995 to the personal security device 930. The computer 900 then employs the key 995 to decrypt the personal security device 930 and gain access to the user's credentials 910, which it then presents to the host 920.

In an alternate embodiment, the personal security device server 940 and the authentication server 980 can be the same server. In another alternate embodiment, the personal security device 930 comprises the user's private key with which the user generates the credentials 910.

Example 2

In this example, as illustrated in FIG. 10, a user wishes to form a secure network connection to a host computer 1000 from a public computer 1010. An example of a public computer is a workstation in a university's computing cluster. The user first obtains a personal security device 1020 containing encrypted information necessary for making a secure network connection, which the user then stores on a non-volatile medium 1030 such as the public computer's disk drive. In this example, the personal

security device 1020 is obtained directly from the host computer 1000, but it may also be obtained from a separate computer such as an authentication server.

The user then applies a key 1040 to decrypt the contents 1050 of the personal security device 1020. The decrypted contents 1050 reside in volatile storage 1060. In this example, the key 1040 is a passphrase that the user has memorized. In an alternative embodiment, the key 1040 is obtained from an authentication token.

In this example, the personal security device 1020 may persist on the public computer, such that a subsequent user is able to read it. However, since the neither the key 1040 nor the decrypted contents 1050 of the personal security device 1020 persist, subsequent users cannot exploit the contents of the personal security device 1020.

Example 3

In this example, as illustrated in FIG. 11, a user with an authentication token 1100 wishes to access the information in a personal security device 1110 stored on the hard disk drive 1120 of the user's computer. When the user wishes to decrypt the information stored in the personal security device 1110, the user queries an authentication server 1130 and presents authentication information 1140 from the authentication token 1100 to the authentication server 1130. Upon receiving proper authentication 1140, the authentication server 1130 then provides the user with a key 1150, which is then used to decrypt the contents 1160 of the personal security device.

In this example, the key 1150 and the decrypted contents 1160 are only maintained in volatile RAM 1170 and never written out to non-volatile disk 1120. Thus when the user turns off or resets the computer 1180, the key 1150 and decrypted contents 1160 are no longer accessible on the computer 1180. If the user wishes to access the contents 1160 of the personal security device 1110 again after cycling the power or resetting the computer 1180, the user has to repeat the authentication process described above. In a further embodiment, the key 1150 and decrypted contents 1160 are removed from volatile RAM 1170 when they are no longer being used. For example, the volatile RAM 1170 containing the key 1150 is zeroed out after decryption is complete, and the

-21-

volatile RAM 1170 containing the decrypted contents 1160 is zeroed out after the user is finished with it.

If the user's computer 1180 is stolen or otherwise physically compromised, an adversary cannot exploit the contents of the personal security device 1110.

Example 4

In this example, as illustrated in FIG. 12, a user with a smartcard 1200 wishes to perform an authentication function. The smartcard includes volatile 1210 and non-volatile 1220 memory. A personal security device 1230 is stored in the smartcard's non-volatile memory 1220. The smartcard 1200 receives power when it is inserted into a smartcard reader 1240; when the smartcard 1200 is removed from the reader 1240, the contents of its volatile memory 1210 are lost. The user inserts the smartcard 1200 into the reader 1240 and provides the reader 1240 with a key such as a PIN 1250.

The PIN 1250 is used to decrypt the personal security device 1230. The decrypted contents 1260 are stored in the smartcard's volatile memory 1210, which the user employs for authentication functions such as digital signatures. When finished, the user removes the smartcard 1200 from the card reader 1240, erasing the sensitive contents 1260 stored in the smartcard's volatile memory 1210.

If the smartcard 1200 is lost or stolen, the information in its personal security device 1230 cannot be exploited by a finder or thief.

Example 5

In this example, as illustrated in FIG. 13, the personal security device 1300 is stored in non-volatile external storage device 1310, which is in operative association with an interface 1320 of a computer 1330. The interface 1320 is in operative association with a central processing unit ("CPU") 1340, which is in operative association with a volatile storage medium 1350. The key 1360 to the personal security device 1300 is stored in the volatile storage medium 1350. The decrypted contents 1370 of the personal security device 1300 is stored in the volatile storage medium 1350.

In one embodiment, the non-volatile external storage device 1310 is a cartridge storing the personal security device 1300 in read only memory ("ROM"). In a further embodiment, the non-volatile external storage device 1300 is a Personal Computer Memory International Association ("PCMCIA") card and the interface 1320 is a

5   PCMCIA slot. In an alternate embodiment, the non-volatile external storage device 1300 is a universal serial bus ("USB") key and the interface 1320 is a USB port. In another alternate embodiment, the non-volatile external storage device 1300 is a card with a magnetic strip and the interface 1320 is a magnetic card reader. In yet another alternate embodiment, the non-volatile external storage device 1300 is a disk and the interface

10   1320 is a disk drive. In a further embodiment, the disk is a floppy disk and the disk drive is a floppy disk drive. In an alternate further embodiment, the disk is a CD-ROM and the disk drive is a CD-ROM drive. In another alternate embodiment, the disk is a Zip disk and the disk drive is a Zip drive.

Equivalents

15   The invention may be embodied in other specific forms without departing from the spirit or essential characteristics thereof. The foregoing embodiments are therefore to be considered in all respects illustrative rather than limiting on the invention described herein. Scope of the invention is thus indicated by the appended claims rather than by the foregoing description, and all changes which come within the meaning and range of

20   equivalency of the claims are therefore intended to be embraced therein.